

明 細 書

サービス提供装置、サービス提供プログラム、コンピュータ読み取り可能な記録媒体、サービス提供方法、およびキーユニット

技術分野

[0001] 本発明は、ID認証を用いて、ユーザに最適なサービスを提供し得るサービス提供システムに関する。

背景技術

[0002] サービス提供システムの一例としての防犯システムに係る分野においては、様々な防犯手法が提案されている。その中でも特に多い手法は、監視カメラを用いて防犯を行う手法である。

[0003] たとえば、特許文献1(特開2003-199088号公報, 2003年07月11日公開)においては、図8に示すように、撮影装置100と、撮影装置100で撮影された映像情報をインターネット110上に送信する住宅側端末120と、その映像情報をインターネット110上から受信して移動端末局130へ送信するホストコンピュータ140とを備え、住宅側端末120やホストコンピュータ140が訪問客などを捕捉すると、ホストコンピュータ140から移動端末局130に映像情報が送信される構成が開示されている。

[0004] また、特許文献2(特開2002-312865号公報, 2002年10月25日公開)においては、図9に示すように、ドア200に接近した来訪者を外部ユニット210に設けられた赤外線センサ等の人物検知装置が検知すると、撮像装置220がONとなり、その旨および撮像された画像が録画されていることを、画像表示手段230を介して文字情報により、あるいはスピーカ240を介して音声情報により示す構成について開示されている。

発明の開示

[0005] しかしながら、上記従来技術には、家屋に近づく者が誰であるかを特定することなく撮像装置により監視領域の撮影を行うので、防犯が必要無いような状況においても不必要に防犯システムが動作してしまう問題がある。

[0006] 具体的には、従来技術では、家屋に近づく者が誰であるかを判断しないので、家

屋に近づく者がその家屋の家人、新聞等の配達者、近隣の住人であるか否かに関わらず防犯システムを動作させる。

[0007] たとえば、その家屋の家人が帰宅する場合には、撮像装置により家人を撮影して防犯体制をとる必要はあまりない。さらに、家人が帰宅した場合に防犯システムが動作していると、その家人は防犯システムを解除するか、あるいは在宅時の設定にするなどの必要があり、却って家人に煩わしささえ感じさせる場合もある。

[0008] また、新聞等の配達者、近隣の住人など、家屋内に不法侵入する可能性が低い者が、家屋のドアに近づいた場合にまで防犯システムを動作させることは、あまり効率的な防犯であるとはいえない。さらに、マンション等の集合住宅などにおいて、特許文献2に記載の技術のように撮像装置による撮影が行なわれていることを、スピーカを用いて音声情報により示すと、近隣住人がドアの前を通過する度に音声メッセージが流れることとなり、却って近所迷惑である。

[0009] 本発明は、上記従来の問題点に鑑みなされたものであって、より効率的な防犯を行うことを可能とし、さらには種々のサービス提供にも応用し得るサービス提供装置、サービス提供方法、サービス提供プログラム、コンピュータ読み取り可能な記録媒体、キーユニットを提供することを目的とする。

[0010] 本発明のサービス提供装置は、上記目的を達成するために、ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、当該サービス提供装置の動作を制御する制御手段とを備え、上記制御手段は、上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのID認証を行うID認証手段と、上記ID認証手段のID認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備えていることを特徴としている。

[0011] 上記構成によれば、操作検知センサによりユーザがアクセスポイントを操作したと判断される場合に、ID認証手段によりユーザのID認証を行うことができる。そして、ID認証手段によるID認証の結果に応じた外部処理を外部処理決定手段により外部装置に実行させることができる。

- [0012] これにより、たとえば操作の対象物を家屋の玄関ドアとし、アクセスポイントを玄関のドアノブとすれば、家屋内に入る際には必ずドアノブを操作することが必要となるので、家屋内に入る者に対し確実にID認証を行うことが可能となる。そしてそのID認証の結果に応じて、家屋内に設けられた外部装置としての警報装置や通報装置に、サービスとしてID認証結果に基づく防犯処理を実行させることができる。
- [0013] たとえば、ドアノブを操作した者からID認証により正当なID情報を得ることができなかった場合は、上記の警報装置により警報を鳴動させたり、通報装置により家屋への不正侵入がなされている可能性が高い旨を所定の通報先に通報したりできる。一方、ドアノブを操作した者からID認証の結果正当なID情報を得ることができた場合には、その家屋の家人が帰宅したものと判断し、外部装置としての警報装置や通報装置の動作を無効化するというサービスも外部処理決定手段により実行することができる。
- [0014] このように、本発明によれば、ユーザが操作対象物を操作したことをトリガとしてID認証を行い、そのID認証結果に応じて外部装置により外部処理が実行されることとなる。したがって、本発明では、ユーザが単に操作対象物の前を通過するというだけでは外部処理は実行されない。よって、従来のように近隣住人等がドアの前を通過するだけで警報メッセージが流れてしまうという煩わしさを解消できるという効果を奏する。また、家人が帰宅した際には、本発明により自動的に防犯システムを解除することもできるので、従来のように帰宅する度に防犯システムを解除する必要があったという家人の煩わしさも解消することもできるという効果を奏する。
- [0015] さらに、本発明では、ID認証手段がアクセスセンサの判断結果に基づいてユーザのID認証を行うので、アクセスセンサにより操作対象物の周辺にユーザが存在していると判断される場合にユーザのID認証を行うことができる。したがって、操作対象物の周辺にユーザが存在していないと判断されるような場合においてはID認証を行わないように構成できる。したがって、より効率的にユーザのID認証を行い、外部装置にサービスを実行させることが可能となる。
- [0016] このように、本発明によれば、効率的に不正侵入者に対する防犯を行うことができる。さらに、本発明によれば、発明を実施するための形態において後述するように、操

作対象物をユーザが操作したことをトリガとして、ユーザに応じた種々のサービスを実行することができ、操作対象物を操作する際のユーザの満足度を高めることもできるという効果も奏する。

- [0017] 本発明のさらに他の目的、特徴、および優れた点は、以下に示す記載によって十分わかるであろう。また、本発明の利益は、添付図面を参照した次の説明で明白になるであろう。

図面の簡単な説明

- [0018] [図1]本発明のサービス提供装置の一実施形態に係るセキュリティ管理装置の構成を示すブロック図である。
- [図2]図1のセキュリティ管理装置を用いる防犯システムの概要を示す図である。
- [図3]図2の防犯システムにおいて用いられるID認証端末の構成を示すブロック図である。
- [図4]ID認証端末の好適な構成の一例であるキーユニットの構成を示すブロック図である。
- [図5]図1のセキュリティ管理装置における操作検知センサの好適な構成としてのドアノブセンサの構成を示すブロック図である。
- [図6]図1のセキュリティ管理装置により実行される処理の流れを示すフローチャートである。
- [図7]図1のセキュリティ管理装置により実行される処理の流れを示すフローチャートである。
- [図8]従来の防犯システムの一例を示す図である。
- [図9]従来の防犯システムの他の例を示す図である。

発明を実施するための最良の形態

- [0019] [1. システムの概要]

本発明のサービス提供装置の一実施形態としてのセキュリティ管理装置を用いる防犯システムの概要について、図2を用いて説明する。

- [0020] 図2に示すように、本実施形態の防犯システムは、セキュリティ管理装置1と、ID認証端末2と、操作検知センサ3と、アクセスセンサ4と、外部装置5とを含んでいる。

- [0021] セキュリティ管理装置1は、家屋6内に設置されるとともに、ユーザにより携帯されるID認証端末2との間で近距離無線通信を行うことによって、ID認証端末2に記憶されたユーザのID情報や属性情報を取得し、ID認証を行うものである。上記の近距離無線通信としては、周波数が2.4GHz(ギガヘルツ)の無線LAN規格に基づく通信方式や、Blue-Tooth(登録商標)規格の微弱電波を用いた通信方式を用いることができる。なお、セキュリティ管理装置1の構成および機能については後述する。
- [0022] ID認証端末2は、上述のように、自身のユーザを認証するためのユーザ情報として、ユーザが誰であるのかを特定するためのID情報や、ユーザの属性を示す属性情報を記録するものである。このID認証端末2は、ユーザが簡易に携帯できるとともにユーザ情報を記録可能な媒体、たとえばICカード、携帯電話機等を用いることが好ましい。
- [0023] また、ID情報としては、ユーザの氏名そのものに関する情報、あるいはユーザの氏名を暗号化した情報を用いることができる。また、属性情報としては、ユーザの性別、年齢、身長、体重、体調等を示す情報を用いることができる。なお、ID認証端末2の構成および機能については後述する。
- [0024] 操作検知センサ3は、ユーザが玄関ドア7のドアノブ8(アクセスポイント)に手を触れたか否か、または手を近づけたか否かを検知するためのものである。操作検知センサ3としては、ユーザ操作によるドアノブ8の振動を検知する振動検知センサ、静電容量の変化を検知する接触センサなどを用いることができる。この操作検知センサ3により、ユーザのドアノブ8に対する操作が検知されたことがトリガとなって、セキュリティ管理装置1によるID認証が実行される。
- [0025] アクセスセンサ4は、ユーザがドアノブ8を操作しているときに存在し得る領域(アクセスエリア、近傍領域)に接近したか否かを検知するためのものである。アクセスセンサ4は、数m半径の領域内における人体の存否を確認するセンサ、たとえば焦電センサ、マイクロ波センサ、超音波ドップラセンサを用いることができる。
- [0026] 外部装置5は、家屋内における警報装置、通報装置、テレビジョンなどの画像表示装置、エアコン等、セキュリティ管理装置1と独立した機器として構成されるものである。さらに、「外部装置」には、家屋外に設置された課金装置、PC端末、携帯電話等の

機器も含まれる。

[0027] 以上のような構成により、セキュリティ管理装置1は、操作検知センサ3によりドアノブ8にユーザが触れたことが検知された場合に、ユーザが有するID認証端末2を用いてID認証を行い、その結果に基づき、外部装置5に対し外部処理命令を与え、種々の処理を実行することを命令する。以下、上述した防犯システムを構成する要素のそれぞれについて、構成および機能を詳細に説明する。

[0028] [2. ID認証端末の構成]

まず、ID認証端末2の構成および機能について説明する。図3に示すように、ID認証端末2は、通信部10と、ユーザ情報記録部11と、制御部12とを備えている。

[0029] 通信部10は、外部装置との通信を行うためのインターフェース回路であり、セキュリティ管理装置1との通信を実現するものである。たとえば、ID認証端末2がICカードであれば、リーダライタとしてのセキュリティ管理装置1が放出するエネルギーの一部を、電源として利用するアンテナコイルにより通信部10は実現される。また、ID認証端末2が携帯電話機であれば、通信部10は、携帯電話機において携帯電話通信を実現する通信回路により実現される。

[0030] ユーザ情報記録部11は、ID認証端末2のユーザを認証するためのユーザ情報として、上述したID情報および属性情報を記録するものである。ここで、ID情報は、ユーザが誰であるのかを特定することができる情報であるので、プライバシー保護および不正利用防止の観点から、一旦ユーザ情報記録部11に書き込まれた後は変更できないようにしておくことが好ましい。したがって、ユーザ情報記録部11のうちID情報を記録する部分は、フィールド・プログラマブルROMなどの1回のみ書込みが可能な記録媒体によって構成しておき、ID認証端末2を最初に使用開始する際にID情報の記憶処理を行う、という構成をとることが好ましい。

[0031] また、属性情報のうち、ユーザの性別を示す情報は基本的に一生変わることはないが、ユーザの年齢、身長、体重、体調等を示す情報は時々刻々と変化するものである。属性情報は書き換え可能にID認証端末2に記録されていることが好ましい。したがって、ユーザ情報記録部11のうち属性情報を記録する部分は、書き換え可能な記録媒体、たとえばEEPROM(Electrically Erasable Programmable Read Only

Memory)により構成しておくことが好ましい。

[0032] 制御部12は、ID認証端末2における処理を統括的に制御するものである。特に、制御部12は、ユーザ情報記録部11からID情報または属性情報を取得するユーザ情報取得部13を備えている。なお、ユーザ情報取得部13によるユーザ情報の取得は、セキュリティ管理装置1からの通信部10を介したユーザ情報取得要求に基づき実行され、取得されたユーザ情報は、通信部10によりセキュリティ管理装置1に送信される。

[0033] 上記構成により、ID認証端末2は、通信部10によりセキュリティ管理装置1との通信を行うとともに、その通信内容に基づき、ユーザ情報記録部11に記録されたID情報または属性情報をユーザ情報取得部13により読み出す。さらに、ID認証端末2は、通信部10を用いて、ID情報または属性情報をセキュリティ管理装置1に送信する。

[0034] [3. セキュリティ管理装置の構成]

次に、セキュリティ管理装置1の構成および機能について説明する。セキュリティ管理装置1は図1に示すように、通信処理部(無線通信手段)14と、制御部(制御手段)15と、記録部16とを備えている。

[0035] 通信処理部14は、外部機器との通信を行うためのインターフェース回路であり、ID認証端末2との通信を実現するID認証端末通信部(無線通信手段)17と、外部装置との通信を実現する外部装置通信部(無線通信手段)18とを備えている。

[0036] ここで、ID認証端末通信部17とセキュリティ管理装置1との通信は、上述のように近距離無線通信によって実現されているので、ID認証端末通信部17としては、数m程度の近距離無線通信を実現するものであればよい。

[0037] 一方、外部装置通信部18は、通常のケーブルを用いた有線通信を採用しても、近距離の無線通信を採用しても構わない。特に、外部装置が家屋外に設定されたPC端末、携帯電話等の機器である場合、外部装置通信部は、インターネット網や携帯電話網等の広域通信を実現するものであることが好ましい。

[0038] なお、ID認証端末通信部17と、外部装置通信部18とは図1において別ブロックとして記載したが、必ずしもこれらの通信部は別個のものとして構成されている必要はない。すなわち、通信に用いる電波の出力を切り替えることにより通信領域の広狭を

切り替え可能な無線通信手段に、ID認証端末通信部17および外部装置通信部18の役割を負わせることも可能である。

- [0039] つまり、上述のような無線通信手段により低パワーの電波を出力することにより、数m半径内の領域における狭域無線通信を実現すれば、ID認証端末通信部17の機能を同無線通信手段に担保させることができる。一方、同無線通信手段により高パワーの電波を出力することにより、数km半径内の領域における広域通信を実現すれば、外部装置通信部18の役割を同無線通信手段に担保させることも可能である。
- [0040] 制御部15は、セキュリティ管理装置1内部の処理を統括的に制御するものである。特に、制御部15は、操作有無判断部19と、アクセス判断部20と、ID認証処理部(ID認証手段)21と、外部処理決定部(外部処理決定手段)22とを備えている。
- [0041] 操作有無判断部19は、ドアノブ8に対するユーザの操作が操作検知センサ3により検知されたか否かを判断するものである。また、アクセス判断部20は、ドアノブ8の近辺における人物の存在がアクセスセンサ4により検知されたか否かを判断するものである。
- [0042] ID認証処理部21は、通信処理部14を介してID認証端末2と通信を行うことにより、ID認証処理を実行するものである。具体的には、ID認証処理部21は、ID認証端末2のユーザ情報記録部11に格納されたID情報を取得し、そのID情報と、セキュリティ管理装置1の記録部16に記録された許可ID情報とを比較することによってID認証処理を行う。
- [0043] すなわち、セキュリティ管理装置1の記録部16に記録された許可ID情報は、家屋内における居住者およびその友人、親戚等、家屋内に居ることが許可された者のIDを示す情報である。したがって、ID認証処理部21は、ID認証端末通信部17を介して取得したID情報が許可ID情報に含まれているか否かを判断することによって、ID認証端末2が正当なID情報を有しているか否かを判断することができる。
- [0044] なお、ユーザのID認証処理は、上述のようにID認証端末2におけるID情報を取得して行う方式に限定されるものではない。たとえば、バイOMETリックな手段、すなわち指紋認識、顔面認識、網膜認識、虹彩認識、音声認識などの手段をセキュリティ管理装置1に設け、これによってユーザの認証を行うことも可能である。

[0045] 外部処理決定部22は、操作有無判断部19による判断結果、アクセス判断部20による判断結果、およびID認証処理部21によるID認証結果に基づき、外部装置通信部18を介して、外部装置に外部処理命令を付与するものである。具体的には、外部処理決定部22は、操作有無判断部19によりユーザがドアノブ8を操作したことを判断し、さらにアクセス判断部20によりドアノブ8の近辺に人物が存在すると判断された場合において、ID認証処理部21により得られたID情報や属性情報に応じた処理を実行するよう、外部機器に動作命令を付与する。外部機器が行う動作の詳細については後述する。

[0046] 以上のように、セキュリティ管理装置1は、ユーザが携帯するID認証端末2からユーザのID情報や属性情報を取得してID認証処理部21によりID認証処理を行うとともに、操作有無判断部19およびアクセス判断部20の判断結果を考慮して、外部装置が行う処理を決定するものである。

[0047] [4. 好適なID認証端末の構成]

次に、ID認証端末の好適な実施形態であるキーユニットの構成について説明する。図4に示すように、本実施形態のキーユニット23は、通信部(ID情報送信手段)24と、制御部25と、記録部(記録手段)26と、表示部(表示手段)27とを備えている。さらに、キーユニット23は、鍵穴に差し込まれる鍵部(キー部分)28と、鍵部28を鍵穴に差し込んで開錠・施錠する場合に鍵部28に発生するトルクを検出するトルクセンサ(操作検知センサ)29と、鍵部28を鍵穴に差し込む際に鍵部がキーユニットに付与する力を検出する圧力センサ(操作検知センサ)30とを備えている。

[0048] 通信部24は、キーユニット23と外部機器との通信を行うためのインターフェース回路である。特に、通信部24は、セキュリティ管理装置1との通信を実現するものである。近距離無線通信方式を採用することが好ましい。

[0049] 制御部25は、キーユニット内部の処理を統括的に制御するものである。特に制御部25は、ユーザ情報取得部31と、本体側情報取得部32と、使用検知部33とを備えている。

[0050] ユーザ情報取得部31は、記録部26に記録されたID情報や属性情報を取得するものである。さらに、ユーザ情報取得部31は、記録部26から取得したID情報や属性情

報を、セキュリティ管理装置1のID認証処理部21がID認証に用いることができるよう、これらの情報をセキュリティ管理装置1のID認証処理部21に送信する。

[0051] 本体側情報取得部32は、過去の家屋内における異常履歴を示す異常履歴情報や、現在家屋内に居る者を示す在宅者情報などを、通信部24を介してセキュリティ管理装置1の記録部16から取得するものである。

[0052] なお、異常履歴情報は、セキュリティ管理装置1の制御部15により作成されるものである。具体的には、ID認証処理部21がドアノブ8を操作するユーザから正当なID情報を取得できない場合に、家屋内に不正侵入がなされた可能性が高い時刻を示す情報が、異常履歴情報として作成される。

[0053] また、在宅者情報も、セキュリティ管理装置1の制御部15により作成されるものである。具体的には、制御部15は、ドアノブ8を操作するユーザから正当なID情報を取得できた場合には、その履歴を在宅者情報として作成する。

[0054] 表示部27は、液晶パネル等の画像表示装置により構成されるものであり、本体側情報取得部32が取得した異常履歴情報や在宅者情報を表示するものである。表示部27にてこれらの情報を表示することにより、ユーザは、家屋内における過去の異常履歴や、現在家屋内にいる者を確認することができる。

[0055] 使用検知部33は、トルクセンサ29または圧力センサ30の出力を判断することにより、現在キーユニット23の鍵部28が鍵穴に差し込まれて開錠または施錠に用いられているか否かを判断するものである。

[0056] すなわち、キーユニット23の鍵部28を鍵穴に挿入して開錠する際には、鍵部28が鍵穴を回転させることになるので、鍵部28にはトルクが発生することになる。したがって、トルクセンサ29によりキーユニット23が使用されているか否かを判断することができる。また、キーユニット23を鍵穴に挿入する際には、鍵部28を鍵穴に押し当てる力が発生するので、その反力を圧力センサ30により検出すれば、キーユニット23が使用されているか否かを判断することができる。

[0057] この使用検知部33は、上述した操作検知センサ3としても機能するものである。すなわち、キーユニット23の鍵部28を鍵穴に差し込む際には、同時にドアノブに手を近づけることにもなる。したがって、使用検知部33によりキーユニット23の使用があっ

たか否かを判断すれば、ユーザがドアノブ8に手を近づけたか否かを判断することができる。

[0058] このようにキーユニット23に使用検知部33を設けることにより、キーユニット23は、ID認証端末2としての機能と、操作検知センサ3としての機能とを有することとなる。つまり、本実施形態のキーユニット23では、ID認証端末2と操作検知センサ3とが一体的に構成されているので、特にドアノブ8に操作検知センサ3を設ける必要がなくなる。したがって、本実施形態の防犯システムをより低コストにて提供することができる。

[0059] [5. ドアノブセンサ]

次に、操作検知センサの好適な実施形態であるドアノブセンサの構成について説明する。図5に示すように、本実施形態のドアノブセンサ40は、ドア41のドアノブ42に取り付けられるコイル43と、発振部(磁界発生手段)44と、検波部(検波手段)45と、判定部46とを備えている。

[0060] 発振部44は、ドアノブ42に取り付けられたコイル43に電流を付与することにより、誘導磁界を発生させるものである。このように発振部44により発せられる誘導磁界の磁力は、ユーザがドアノブ42に手を近づけると変化する。検波部45は、このように生じる磁力の変化を検知するものである。

[0061] そして、判定部46は、検波部45が所定レベル以上の磁力変化を検知したか否かを判断することにより、ユーザがドアノブに手を近づけたか否かを判断するものである。すなわち、ユーザがドアノブに手を近づければ近づくほど、コイル43により発生される磁界には大きな変化が生じる。したがって、判定部46においては、検波部45が所定レベル以上の磁力変化を検知した場合に、ユーザがドアノブに手を近づけたと判断される。

[0062] このように、本実施形態のドアノブセンサ40によれば、ドアノブ42にコイル43を引っ掛けるという簡易な構成により、ユーザがドアノブに手を近づけたか否かを判断できる。したがって、ドアに穴を開けて振動検知センサや接触センサを設けることなく、操作検知センサ3をドアに設けることができるので、低コストにて本実施の形態の防犯システムを提供することができる。

[0063] [6. 処理フロー]

次に、本実施の形態のセキュリティ管理装置1により実行される処理フローについて説明する。なお、セキュリティ管理装置1が実行する処理フローには、アクセスセンサ4の検知結果を用いない場合と用いる場合との2通りの処理フローがあるので、これらの処理フローを順番に説明する。

[0064] (6-1. アクセスセンサの検知結果を用いない場合)

まず、アクセスセンサの検知結果を用いない場合の処理フローを説明する。図6に示すように、セキュリティ管理装置1の制御部25により、セキュリティモードがONに設定される(ステップ1、以下各ステップを単にSと記載する)。

[0065] なお、セキュリティモードとは、後述するように、ID認証端末2に記録されたID情報に基づき、セキュリティを解除したり外部処理を実行したりするモードのことを意味する。

[0066] その後、玄関ドア7が開いたか否かが、操作検知センサ3により検知される(S2)。S2において玄関ドアが開いていないと判断された場合、再度S2に戻り玄関ドアが開いたか否かの判断が行われる。

[0067] S2において玄関ドア7が開いたと判断された場合、ID認証端末通信部17により、ユーザがID認証端末2を有しているか否かが判断される(S3)。具体的には、ID認証端末通信部17が通信可能な通信エリア内にID認証端末2が存在するか否かを判断することにより、S2の判断が行われる。

[0068] S3においてユーザがID認証端末を有していないと判断された場合、ID認証端末を有していない者が玄関ドア7を開けたことになるので、家屋への不正侵入がなされている可能性が高い。そこで、外部処理決定部22は、その判断結果に基づき、外部装置としての警報装置に対し、警報を鳴動する処理を外部処理として行うよう命令する(S4)。

[0069] なお、S4において、外部処理決定部22は、外部装置としての通報装置に対して、不正侵入がなされようとしている旨を所定の通報先へ通報する処理を外部処理として行うよう命令してもよい。特に、不正侵入がなされようとしている旨を通報する際には、上述した通信領域の広狭を切り替え可能な無線通信手段によりID認証端末通信部17と外部装置通信部18との役割を担保させることが有利である。

- [0070] すなわち、当該無線通信手段により、広域の無線通信を行えば、数km先にいるユーザのID認証端末にも不正侵入がなされようとしている旨を通報することができる。これにより、ユーザにより迅速に家屋への不正侵入を知らせることができる。
- [0071] S4の後、S5において、制御部15は記録部16における異常履歴情報を更新する。具体的は、ID認証端末を有していない者が玄関ドアを開けたことと、その者により玄関ドアが開けられた時刻とを異常履歴情報に追加する。この異常履歴情報は、上述したキーユニット23をユーザが携帯している場合に有効に活用される。
- [0072] すなわち、ユーザがキーユニット23(図4参照)を携帯している場合には、異常履歴情報が表示部27において表示されるので、ユーザは家屋内に入る前に、家屋への不正侵入があったか否かを確認できる。したがって、家人と不正侵入者とが鉢合わせして不正侵入者から暴力を受けるというような事故を未然に防止できる。
- [0073] 一方、S3においてユーザがID認証端末を有していると判断された場合、ID認証処理部21により、ID認証端末が正当なID情報を有しているか否かが判断される(S6)。S6においては、たとえば上述したように、ID認証処理部21が、ID認証端末通信部17を介して取得したID情報が許可ID情報に含まれているか否かを判断することによって、ID認証端末が正当なID情報を有しているか否かを判断することができる。
- [0074] S6においてID認証端末が正当なID情報を有していないと判断された場合には、上述したS4における警報の鳴動処理を実行した後、S5において異常履歴情報の更新処理が実行される。
- [0075] また、S6においてID認証端末が正当なID情報を有していると判断された場合には、制御部15により、セキュリティの解除処理が実行される。セキュリティの解除処理とは、家屋内の窓やドアに取り付けられた不正侵入検知用の振動センサや、家屋内に取り付けられた人体検知センサ等の防犯センサの動作を停止させる処理を意味している。
- [0076] S7においてセキュリティの解除処理が行われた後、S8において、外部処理決定部22は、ID認証端末2のID情報に応じた各種の処理を実行するよう、外部装置に外部処理命令を付与する。
- [0077] たとえば、ID認証端末のID情報が子供のものと判断された場合には、外部

処理決定部22は、外部装置としての防犯センサを起動したり、家屋内の玄関、扉、窓等に取り付けられた外部装置としての鍵が施錠されるように、外部処理命令を付与する。これにより、子供が家屋内への不正侵入者に暴行を受ける被害を未然に防ぐことが可能となる。また、ID認証端末のID情報が老人のものである場合にも、同様の外部処理命令が外部処理決定部22により付与される。

[0078] また、家屋内において各個人に部屋が割り当てられている場合には、ID認証端末のID情報からその個人に割り当てられた部屋を判断し、外部装置としてのその部屋の照明が点灯されるよう、外部処理決定部22により外部処理命令を付与してもよい。さらには、外部装置としてのその部屋のエアコンが作動するよう、外部処理決定部22から外部処理命令を付与してもよい。

[0079] (6-2. アクセスセンサの検知結果を用いる場合)

次に、アクセスセンサの検知結果を用いる場合の処理フローを説明する。図7に示すように、セキュリティ管理装置1の制御部25により、セキュリティモードがONに設定される(S11)。

[0080] その後、玄関ドア7の前にユーザが居るか否かが、アクセスセンサ4により判断される(S12)。S12において玄関ドア7の前にユーザが居ないと判断された場合には、再度S12において玄関ドア7の前にユーザが居るか否かが判断される。

[0081] S12においてドアの前にユーザがいると判断された場合には、ID認証端末通信部17により、ユーザがID認証端末2を有しているか否かが判断される(S13)。S13においてユーザがID認証端末2を有していないと判断された場合には、外部処理決定部22は、外部装置としての警報装置に対し、1次警報処理を行うよう命令する(S14)。

[0082] ここで、1次警報処理とは、家屋への不正侵入がなされようとしている可能性があることを、警報装置により警報を鳴動させることによってユーザに知らせる処理のことをいう。すなわち、S13において玄関ドアの前に居るユーザがID認証端末2を有していないと判断されたことは、その家屋の家人以外の者が玄関ドアの前に立っているということなので、家屋への不正侵入がなされようとしている可能性が高いと判断できる。

[0083] ただし、新聞や郵便の配達者が玄関ドアの前に立っている場合に大音量の警報が

鳴動されてしまつては、近所迷惑となつてしまう場合がある。したがって、1次警報処理においては、比較的小音量の警報を鳴動させることが好ましい。また、S12においてドアの前にユーザが居ると判断されてから所定時間を経過するまでに、S13においてユーザのID認証端末が認識されない場合に、S14において1次警報処理を実行するようにしてもよい。

[0084] 一方、S13においてユーザがID認証端末を有していると判断された場合は、S15において、そのユーザが玄関ドア7を開けたか否かが操作検知センサ3により判断される(S15)。S15においてドアを開けていないと判断される場合は、再度S12において玄関ドアの前にユーザがいるか否かの判断が行われる。

[0085] 一方、S15においてユーザが玄関ドアを開けたと判断された場合には、S16において、ID認証処理部21により、ID認証端末が正当なID情報を有しているか否かが判断される。S16は、図6のS6と同様の処理であるので、その詳細な説明は省略する。

[0086] S16においてID認証端末が正当なID情報を有していないと判断された場合、S17において、外部処理決定部22は、外部装置としての警報装置に対し、2次警報処理を行うよう命令する(S17)。

[0087] S17における2次警報処理とは、図6のS4と同様の処理である。すなわち、2次警報処理とは、外部装置としての警報装置が警報を鳴動させる処理や、通報装置が所定の通報先に不正侵入がなされようとしている旨を通報する処理のことを意味している。

[0088] なお、この2次警報処理が行われる場合は、正当なID認証端末を有していないユーザが既に家屋内に入ってきている場合なので、家屋への不正侵入が行われている可能性が非常に高い。したがって、2次警報処理においては、より大音量で警報を鳴動させたり、所定の通報先に不正侵入を通報する処理を行うことにより、不正侵入した者に対する威嚇をより効果的に行うことができる。

[0089] さらに、S17の後、S18において、制御部15は記録部16における異常履歴情報を更新する。S18の処理は、図6のS5の処理と同様であるのでその詳細な説明は省略する。

[0090] 一方、S16においてID認証端末が正当なID情報を有していると判断された場合、

S19において、制御部15により、セキュリティの解除処理が実行された後、S20において、外部処理決定部22により、ID認証端末2のID情報に応じた各種の処理を実行する命令が外部装置に対してなされる。S19は図6のS7と同一の処理であり、S20は図6のS8と同一の処理であるので、その詳細な説明は省略する。

[0091] [7. 他のサービスへの適用例]

上述の実施形態では、玄関ドアのドアノブをアクセスポイントとし、そのアクセスポイントをユーザが操作した場合、すなわちアクセスポイントにユーザがアクセスした場合に、ユーザのID認証を行い、そのID認証結果に基づき外部処理が行われる。しかしながら、本発明のサービス提供装置の適用範囲は上述したような防犯システムのみに限られるものではない。

[0092] たとえば、本発明のサービス提供装置は、工作機械の操作説明システムにも用いることができる。すなわち、工作機械の操作部をアクセスポイントとすれば、本発明のサービス提供装置を用いることにより、そのアクセスポイントにユーザがアクセスした場合にユーザのID認証を行い、ユーザのIDに応じた外部処理を行うことができる。

[0093] 具体的には、工作機械の操作部に上述したような操作検知センサを設けておき、その操作検知センサによりユーザが操作部を操作したと判断される場合にユーザのID認証を行う。そして、ユーザのID情報からその工作機械の操作についてユーザがどの程度習熟しているかを判断し、その習熟度に応じた操作説明を工作機械のディスプレイから行う処理を外部処理として実行することができる。たとえば、初心者に対しては、工作機械のディスプレイに操作方法を逐一表示するとともに、音声による操作案内を行うという処理を行うことにより、工作機械の操作について説明することができる。一方、熟練者に対しては、全く操作説明を行わないという処理を行うこともできる。

[0094] また、本発明のサービス提供装置は、PC (Personal Computer) に用いることもできる。すなわち、PCを操作するにあたってユーザが必ずアクセスする箇所、たとえば電源スイッチ、マウス、キーボード等をアクセスポイントとすれば、本発明のサービス提供装置を用いることにより、以下のような外部処理を行うことができる。

[0095] 具体的には、PCの電源スイッチに操作検知センサを設けておき、その操作検知センサによりユーザが電源スイッチを押下したと判断される場合に、ユーザのID認証を

行う。そのID認証により得られたユーザのID情報に基づいて、各ユーザについて設定された起動画面を表示する処理を外部処理として行うことができる。さらに、PC起動時に実行されるプログラムについて、各ユーザが異なる設定をしている場合には、ID認証により得られたユーザのID情報に基づき、そのユーザが設定したプログラムを自動的に実行する処理を外部処理として行うことができる。

[0096] さらに、本発明のサービス提供装置は、料理提供サービスにも用いることができる。すなわち、ユーザが料理をするにあたって必ずユーザがアクセスする箇所、たとえば冷蔵庫の開閉ハンドルをアクセスポイントとすれば、本発明のサービス提供装置を用いることにより、以下のような外部処理を行うことができる。

[0097] 具体的には、冷蔵庫の開閉ハンドルに操作検知センサを設けておき、その操作検知センサによりユーザが開閉ハンドルを操作したと判断される場合にユーザのID認証を行う。そして、ユーザのID情報からユーザの健康状態を判断し、そのユーザの健康状態に最適な食材を選択して冷蔵庫のディスプレイに表示する処理を外部処理として行うことができる。

[0098] また、本発明のサービス提供システムは、レンタカーを利用する際の課金システムに用いることもできる。すなわち、レンタカーを利用するにあたってユーザが必ずアクセスする箇所、たとえばドアハンドルやステアリング等をアクセスポイントとすれば、本発明のサービス提供装置を用いることにより、以下のような外部処理を行うことができる。

[0099] 具体的には、上述のアクセスポイントに操作検知センサを設けておき、その操作検知センサによりユーザがドアハンドル等を操作したと判断される場合、ユーザのID認証を行う。そして、そのID認証により得られるID情報をレンタカー利用料金を管理する管理サーバに送信し、各ユーザについての利用料金を自動課金するということが可能である。

[0100] [8. 補足]

最後に、上記セキュリティ管理装置1の各ブロックは、ハードウェアロジックによって構成してもよいし、次のようにCPUを用いてソフトウェアによって実現してもよい。

[0101] すなわち、セキュリティ管理装置1は、各機能を実現する制御プログラムの命令を実

行するCPU (central processing unit)、上記プログラムを格納したROM (read only memory)、上記プログラムを展開するRAM (random access memory)、上記プログラムおよび各種データを格納するメモリ等の記憶装置 (記録媒体) などを備えている。そして、本発明の目的は、上述した機能を実現するソフトウェアであるセキュリティ管理装置1の制御プログラムのプログラムコード (実行形式プログラム、中間コードプログラム、ソースプログラム) をコンピュータで読み取り可能に記録した記録媒体を、セキュリティ管理装置1に供給し、そのコンピュータ (またはCPUやMPU) が記録媒体に記録されているプログラムコードを読み出し実行することによっても、達成可能である。

- [0102] 上記記録媒体としては、たとえば、磁気テープやカセットテープ等のテープ系、フロッピー (登録商標) ディスク / ハードディスク等の磁気ディスクやCD-ROM / MO / MD / DVD / CD-R等の光ディスクを含むディスク系、ICカード (メモリカードを含む) / 光カード等のカード系、あるいはマスクROM / EPROM / EEPROM / フラッシュROM等の半導体メモリ系などを用いることができる。
- [0103] また、セキュリティ管理装置1を通信ネットワークと接続可能に構成し、上記プログラムコードを通信ネットワークを介して供給してもよい。この通信ネットワークとしては、特に限定されず、たとえば、インターネット、イントラネット、エキストラネット、LAN、ISDN、VAN、CATV通信網、仮想専用網 (virtual private network)、電話回線網、移動体通信網、衛星通信網等が利用可能である。また、通信ネットワークを構成する伝送媒体としては、特に限定されず、たとえば、IEEE1394、USB、電力線搬送、ケーブルTV回線、電話線、ADSL回線等の有線でも、IrDAやリモコンのような赤外線、Bluetooth、802.11無線、HDR、携帯電話網、衛星回線、地上波デジタル網等の無線でも利用可能である。なお、本発明は、上記プログラムコードが電子的な伝送で具現化された搬送波あるいはデータ信号列の形態でも実現され得る。
- [0104] 以上のように、本発明のサービス提供装置は、ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、当該サービス提供装置の動作を制御する制御

手段とを備え、上記制御手段は、上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのID認証を行うID認証手段と、上記ID認証手段のID認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備えているものである。

- [0105] 上記構成によれば、操作検知センサによりユーザがアクセスポイントを操作したと判断される場合に、ID認証手段によりユーザのID認証を行うことができる。そして、ID認証手段によるID認証の結果に応じた外部処理を外部処理決定手段により外部装置に実行させることができる。
- [0106] これにより、たとえば操作の対象物を家屋の玄関ドアとし、アクセスポイントを玄関のドアノブとすれば、家屋内に入る際には必ずドアノブを操作することが必要となるので、家屋内に入る者に対し確実にID認証を行うことが可能となる。そしてそのID認証の結果に応じて、家屋内に設けられた外部装置としての警報装置や通報装置に、サービスとしてID認証結果に基づく防犯処理を実行させることができる。
- [0107] たとえば、ドアノブを操作した者からID認証により正当なID情報を得ることができなかった場合は、上記の警報装置により警報を鳴動させたり、通報装置により家屋への不正侵入がなされている可能性が高い旨を所定の通報先に通報したりできる。一方、ドアノブを操作した者からID認証の結果正当なID情報を得ることができた場合には、その家屋の家人が帰宅したものと判断し、外部装置としての警報装置や通報装置の動作を無効化するというサービスも外部処理決定手段により実行することができる。
- [0108] このように、本発明によれば、ユーザが操作対象物を操作したことをトリガとしてID認証を行い、そのID認証結果に応じて外部装置により外部処理が実行されることとなる。したがって、本発明では、ユーザが単に操作対象物の前を通過するというだけでは外部処理は実行されない。よって、従来のように近隣住人等がドアの前を通過するだけで警報メッセージが流れてしまうという煩わしさを解消できるという効果を奏する。また、家人が帰宅した際には、本発明により自動的に防犯システムを解除することもできるので、従来のように帰宅する度に防犯システムを解除する必要があったという家人の煩わしさも解消することもできるという効果を奏する。

- [0109] さらに、本発明では、ID認証手段がアクセスセンサの判断結果に基づいてユーザのID認証を行うので、アクセスセンサにより操作対象物の周辺にユーザが存在していると判断される場合にユーザのID認証を行うことができる。したがって、操作対象物の周辺にユーザが存在していないと判断されるような場合においてはID認証を行わないように構成できる。したがって、より効率的にユーザのID認証を行い、外部装置にサービスを実行させることが可能となる。
- [0110] このように、本発明によれば、効率的に不正侵入者に対する防犯を行うことができる。さらに、本発明によれば、発明を実施するための形態において後述するように、操作対象物をユーザが操作したことをトリガとして、ユーザに応じた種々のサービスを実行することができ、操作対象物を操作する際のユーザの満足度を高めることもできるという効果も奏する。
- [0111] さらに、上記構成のサービス提供装置において、上記ユーザによる操作の対象物を家屋内へ入るためのドアし、上記アクセスポイントを上記ドアのドアノブとする一方、上記操作検知センサを、上記ドアの開錠に用いられるキーが該ドアを開錠する動作を検知する構成とすることにより、以下の効果が奏される。
- [0112] すなわち、家人が家屋へ入ろうとする際には、施錠されたドアの鍵穴にキーを差し込んでドアを開錠した後、ドアノブを操作することが必要になる。上記構成によれば、操作検知センサはキーがドアを開錠する動作を検知するので、ユーザがキーを用いてドアを開錠したことを的確に検知できる。したがって、ユーザがドアノブを操作することをも的確に検知できる。
- [0113] これにより、ID認証手段によるID認証処理、および外部処理決定手段による外部装置のサービス実行処理が、ユーザのドアノブ操作と確実に連動して行われることとなるので、より効率的な防犯を行うことができるという効果が奏される。
- [0114] なお、キーがドアを開錠する動作を検知する操作検知センサは、たとえば、キーをドアの鍵穴に差し込んだ際にキーの方へ発生する力を検出する圧力センサや、ドアの開錠に用いられるキーを鍵穴に差し込み回転させる際に上記キーに発生するトルクを検出するトルクセンサにより、簡易に実現することができる。
- [0115] さらに上記操作検知センサを、上記ドアノブに設けられるコイルと、上記コイルにより

誘導磁界を発生させる磁界発生手段と、上記磁界発生手段により発生される誘導磁界の磁力変化を検知する検波手段とを備えている構成とすることにより、以下の効果が奏される。

- [0116] すなわち、上記構成によれば、コイルおよび磁界発生手段により、ドアノブの周囲に誘導磁界を発生させることができる。そして、ユーザがドアノブを操作しようとしてドアノブに手を近づけた場合、ドアノブ周囲に発生された誘導磁界に磁力変化が生じるが、この磁力変化を検波手段により検知することができる。
- [0117] このように、上記構成の操作検知センサによれば、ユーザのドアノブに対する操作を的確に検知することができる。したがって、ID認証手段によるID認証処理、および外部処理決定手段による外部装置のサービス実行処理が、ユーザのドアノブ操作と確実に連動して行われることとなるので、より効率的な防犯を行うことができるという効果が奏される。
- [0118] さらに、上記構成のサービス提供装置において、通信に用いる電波の出力を切り替えることにより通信可能領域の広狭を切り替え可能な無線通信手段を設け、上記ID認証手段を、ユーザにより携帯されるID認証端末と上記無線通信手段を用いて狭域無線通信を行うことにより上記ID認証端末から取得されたID情報が、上記サービス提供装置に記録された許可ID情報に含まれているか否かを判断することによって、ユーザのID認証を行う一方、上記無線通信手段を介して正当なID情報を取得できない場合、上記無線通信手段を用いて広域無線通信を行うことにより、正当なID情報を取得できないことを示す情報を外部装置に送信する構成とすることにより、以下の効果が奏される。
- [0119] すなわち、上記構成によれば、無線通信手段により狭域無線通信を行ってユーザのID認証端末からユーザのID情報を取得し、その情報がサービス提供装置に記録された許可ID情報に含まれているか否かという簡易な処理により、ユーザ認証を行うことができるという効果が奏される。なお、許可ID情報とは、操作対象物を操作することが許可されたユーザのIDが格納されている情報を意味する。また、狭域無線通信とは、数m半径内の無線通信を指す意味において用いている。
- [0120] また、ID認証端末から正当なID情報を取得できない場合には、無線通信手段によ

り広域無線通信を行って、外部装置に正当なID情報を取得できないことを示す情報を送信するので、操作対象物の操作を許可されていない者が操作対象物を不正に操作しようとしていることを外部装置に連絡することができる。これにより、外部装置においては、不正操作がなされようとしている場合における所定の処理、たとえば外部への通報処理や警報の鳴動処理を実行することができる。なお、広域無線通信とは、数km半径内の無線通信を指す意味において用いている。

[0121] このように、本発明によれば、ID認証処理と、操作対象物に対する不正操作を外部装置に連絡する処理とを、無線通信手段により通信可能領域の広狭を切り替えて行うことができる。したがって、サービス提供装置の構成をより簡易にすることができるとともに、ユーザの利便性を高めることができるという効果が奏される。

[0122] さらに、本発明のサービス提供方法は、ユーザによる操作の対象物におけるアクセスポイントをユーザが操作したか否かを、サービス提供装置の操作検知センサにより判断する第1ステップと、上記操作検知センサの判断結果に基づくユーザのID認証を、上記サービス提供装置のID認証手段により行う第2ステップと、上記ID認証手段のID認証結果に応じたサービスを、上記サービス提供装置の外部処理決定手段により外部装置に実行させる第3ステップとを備えている。

[0123] 上記のサービス提供方法においては、第1ステップから第3ステップの各ステップにおいて、本発明のサービス提供装置と同一の処理が実現されている。よって、本発明のサービス提供装置と同様の作用効果を得ることができる。

[0124] また、本発明のキーユニットは、以上のように、ドアの鍵穴に差し込まれるキー部分と、ユーザのID情報を記録する記録手段と、上記キー部分が上記ドアの鍵穴に差し込まれることを検知する操作検知センサと、上記操作検知センサの検知結果に基づき、上記記録手段からユーザのID認証を行う外部のID認証手段に、上記ユーザのID情報を送信するID情報送信手段とを備えていることにより、以下の効果を奏する。

[0125] すなわち、上記構成によれば、ユーザがドアを開錠するためにキー部分を差し込むと、操作検知センサによりキー部分が鍵穴に差し込まれたことが検知され、ID情報送信手段により記録手段からユーザのID情報が送信される。

[0126] ここで、上記のID認証手段を、上述した本発明のサービス提供装置におけるものと

することにより、ユーザがドアを開錠するための一連の動作において、自動的にID情報がキーユニットからID認証手段に送信され、ID認証が行われることとなる。したがって、ユーザにおいては、ドアを開錠する以外に余分な動作を行わなくても、サービス提供装置にID認証を実行させることができる。よって、本発明のサービス提供装置に用いるのに適したキーユニットを提供することができるという効果が奏される。

[0127] さらに、上記構成のキーユニットにおいて、上記ID認証手段が行ったID認証の結果に基づき作成される、家屋への不正侵入がなされた可能性が高い時刻を示す異常履歴情報および家屋内に在宅している者を示す在宅者情報の少なくとも一方を、上記ID認証手段から取得し表示する表示手段を備えることにより、以下の効果が奏される。

[0128] すなわち、上記構成によれば、ユーザは、キーユニットの表示手段に表示された異常履歴情報または在宅者情報を確認することにより、家屋への不正侵入がなされた可能性や、現在家屋内に在宅している者を知ることができる。なお、異常履歴情報は、ID認証手段がキーユニットの記録手段から正当なID情報を取得できなかった場合、その履歴を記録しておくことにより作成される。また、在宅者情報はID認証手段がキーユニットの記録手段から正当なID情報を取得した場合、その履歴を記録しておくことにより作成される。

[0129] したがって、ユーザは、家屋に入る前に、現在家屋内にどのような者が居るのかを判断することができるので、不正侵入者と鉢合わせして暴行を受けてしまうという事故を防止することができるという効果が奏される。

[0130] また、本発明のサービス提供プログラムは、上記構成におけるサービス提供装置における制御手段としてコンピュータを機能させるものである。また、本発明のコンピュータ読み取り可能な記録媒体は、上記サービス提供プログラムを格納したものである。これにより、任意のコンピュータ上で上記サービス提供プログラムを実行させることができる。

[0131] 尚、発明を実施するための最良の形態の項においてなした具体的な実施態様または実施例は、あくまでも、本発明の技術内容を明らかにするものであって、そのような具体例にのみ限定して狭義に解釈されるべきものではなく、本発明の精神と特許請

求の範囲内で、いろいろと変更して実施することができるものである。

産業上の利用の可能性

- [0132] 以上のように、本発明のサービス提供装置は、効率的に不正侵入者に対する防犯を行うのに適している。さらに、本発明のサービス提供装置は、防犯システムのみならず、工作機械の操作説明サービス、自動的にPCの起動時設定を変更するサービス、料理提供サービス、レンタカーの課金サービスなど、種々のサービス分野においてユーザに適したサービスを提供するのにも適している。

請求の範囲

- [1] ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、
上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、
当該サービス提供装置の動作を制御する制御手段とを備え、
上記制御手段は、
上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのID認証を行うID認証手段と、
上記ID認証手段のID認証結果に応じたサービスを外部装置に実行させる外部処理決定手段とを備えていることを特徴とするサービス提供装置。
- [2] 上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、
上記アクセスポイントは、上記ドアのドアノブである一方、
上記操作検知センサは、上記ドアの開錠に用いられるキーが該ドアを開錠する動作を検知することを特徴とする請求の範囲第1項に記載のサービス提供装置。
- [3] 上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、
上記アクセスポイントは、上記ドアのドアノブである一方、
上記操作検知センサは、上記ドアの開錠に用いられるキーが該ドアの鍵穴に差し込まれる際に、上記鍵穴から上記キーの方へ発生する力を検出する圧力センサであることを特徴とする請求の範囲第1項に記載のサービス提供装置。
- [4] 上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、
上記アクセスポイントは、上記ドアのドアノブである一方、
上記操作検知センサは、上記ドアの開錠に用いられるキーを鍵穴に差し込み回転させる際に上記キーに発生するトルクを検出するトルクセンサであることを特徴とする請求の範囲第1項に記載のサービス提供装置。
- [5] 上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、
上記アクセスポイントは、上記ドアのドアノブである一方、
上記操作検知センサは、

上記ドアノブに設けられるコイルと、

上記コイルにより誘導磁界を発生させる磁界発生手段と、

上記磁界発生手段により発生される誘導磁界の磁力変化を検知する検波手段とを備えていることを特徴とする請求の範囲第1項ないし第4項のいずれか1項に記載のサービス提供装置。

- [6] 通信に用いる電波の出力を切り替えることにより通信可能領域の広狭を切り替え可能な無線通信手段を備え、

上記ID認証手段は、ユーザにより携帯されるID認証端末と上記無線通信手段を用いて狭域無線通信を行うことにより上記ID認証端末から取得されたID情報が、上記サービス提供装置に記録された許可ID情報に含まれているか否かを判断することによって、ユーザのID認証を行う一方、

上記無線通信手段を介して正当なID情報を取得できない場合、上記無線通信手段を用いて広域無線通信を行うことにより、正当なID情報を取得できないことを示す情報を外部装置に送信することを特徴とする請求の範囲第1項ないし第5項のいずれか1項に記載のサービス提供装置。

- [7] 請求の範囲第1項ないし第6項のいずれか1項に記載のサービス提供装置における制御手段としてコンピュータを機能させることを特徴とするサービス提供プログラム。

- [8] 請求の範囲第7項に記載のサービス提供プログラムを格納したことを特徴とするコンピュータ読み取り可能な記録媒体。

- [9] ユーザによる操作の対象物におけるアクセスポイントをユーザが操作したか否かを、サービス提供装置の操作検知センサにより判断する第1ステップと、

上記操作検知センサの判断結果に基づくユーザのID認証を、上記サービス提供装置のID認証手段により行う第2ステップと、

上記ID認証手段のID認証結果に応じたサービスを、上記サービス提供装置の外部処理決定手段により外部装置に実行させる第3ステップとを備えていることを特徴とするサービス提供方法。

- [10] ドアの鍵穴に差し込まれるキー部分と、

ユーザのID情報を記録する記録手段と、
上記キー部分が上記ドアの鍵穴に差し込まれることを検知する操作検知センサと、
上記操作検知センサの検知結果に基づき、上記記録手段からユーザのID認証を行う外部のID認証手段に、上記ユーザのID情報を送信するID情報送信手段とを備えていることを特徴とするキーユニット。

- [11] 上記ID認証手段が行ったID認証の結果に基づき作成される、家屋への不正侵入がなされた可能性が高い時刻を示す異常履歴情報および家屋内に在宅している者を示す在宅者情報の少なくとも一方を、上記ID認証手段から取得し表示する表示手段を備えていることを特徴とする請求の範囲第10項に記載のキーユニット。

補正書の請求の範囲

JP2004/016152

補正書の請求の範囲〔2005年3月7日（07.03.05）国際事務局受理：出願当初の請求の範囲1及び9は補正された；出願当初の請求の範囲10及び11は取り下げられた；新たな請求の範囲12及び13が追加された；他の請求の範囲は変更なし。（3頁）〕

1. （補正後）ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、

上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、

当該サービス提供装置の動作を制御する制御手段とを備え、

上記制御手段は、

上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザのID認証を行うID認証手段と、

上記操作検知センサの判断結果、上記アクセスセンサの判断結果、および上記ID認証手段のID認証結果の少なくとも1つに応じて、複数のサービスから1つを選択して外部装置に実行させる外部処理決定手段とを備えていることを特徴とするサービス提供装置。

2. 上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、

上記アクセスポイントは、上記ドアのドアノブである一方、

上記操作検知センサは、上記ドアの開錠に用いられるキーが該ドアを開錠する動作を検知することを特徴とする請求の範囲第1項に記載のサービス提供装置。

3. 上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、

上記アクセスポイントは、上記ドアのドアノブである一方、

上記操作検知センサは、上記ドアの開錠に用いられるキーが該ドアの鍵穴に差し込まれる際に、上記鍵穴から上記キーの方へ発生する力を検出する圧力センサであることを特徴とする請求の範囲第1項に記載のサービス提供装置。

4. 上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、

上記アクセスポイントは、上記ドアのドアノブである一方、

上記操作検知センサは、上記ドアの開錠に用いられるキーを鍵穴に差し込み回転させる際に上記キーに発生するトルクを検出するトルクセンサであることを特徴とする請求の範囲第1項に記載のサービス提供装置。

5. 上記ユーザによる操作の対象物は、家屋内へ入るためのドアであり、

上記アクセスポイントは、上記ドアのドアノブである一方、
上記操作検知センサは、
上記ドアノブに設けられるコイルと、
上記コイルにより誘導磁界を発生させる磁界発生手段と、
上記磁界発生手段により発生される誘導磁界の磁力変化を検知する検波手段とを備えていることを特徴とする請求の範囲第1項ないし第4項のいずれか1項に記載のサービス提供装置。

6. 通信に用いる電波の出力を切り替えることにより通信可能領域の広狭を切り替え可能な無線通信手段を備え、

上記ID認証手段は、ユーザにより携帯されるID認証端末と上記無線通信手段を用いて狭域無線通信を行うことにより上記ID認証端末から取得されたID情報が、上記サービス提供装置に記録された許可ID情報に含まれているか否かを判断することによって、ユーザのID認証を行う一方、

上記無線通信手段を介して正当なID情報を取得できない場合、上記無線通信手段を用いて広域無線通信を行うことにより、正当なID情報を取得できないことを示す情報を外部装置に送信することを特徴とする請求の範囲第1項ないし第5項のいずれか1項に記載のサービス提供装置。

7. 請求の範囲第1項ないし第6項のいずれか1項に記載のサービス提供装置における制御手段としてコンピュータを機能させることを特徴とするサービス提供プログラム。

8. 請求の範囲第7項に記載のサービス提供プログラムを格納したことを特徴とするコンピュータ読み取り可能な記録媒体。

9. (補正後) ユーザによる操作の対象物におけるアクセスポイントをユーザが操作したか否かを、サービス提供装置の操作検知センサにより判断する第1ステップと

、
上記操作検知センサの判断結果に基づくユーザのID認証を、上記サービス提供装置のID認証手段により行う第2ステップと、

上記操作検知センサの判断結果、上記アクセスセンサの判断結果、および上記ID

認証手段の I D 認証結果の少なくとも 1 つに応じて、上記サービス提供装置の外部処理決定手段により複数のサービスから 1 つを選択して外部装置に実行させる第 3 ステップとを備えていることを特徴とするサービス提供方法。

10. (削除)

11. (削除)

12. (追加) ユーザによる操作の対象物におけるアクセスポイントを、ユーザが操作したか否かを判断する操作検知センサと、

上記アクセスポイントを操作しているときにユーザが存在し得る近傍領域にユーザが存在するか否かを判断するアクセスセンサと、

当該セキュリティ管理装置の動作を制御する制御手段とを備え、

上記制御手段は、

上記アクセスセンサおよび上記操作検知センサの判断結果に基づき、ユーザの I D 認証を行う I D 認証手段と、

上記操作検知センサの判断結果、上記アクセスセンサの判断結果、および上記 I D 認証手段の I D 認証結果の少なくとも 1 つに応じて、複数の警報処理から 1 つを選択して外部装置に実行させる外部処理決定手段とを備えていることを特徴とするセキュリティ管理装置。

13. (追加) ユーザによる操作の対象物におけるアクセスポイントをユーザが操作したか否かを、セキュリティ管理装置の操作検知センサにより判断する第 1 ステップと、

上記操作検知センサの判断結果に基づくユーザの I D 認証を、上記セキュリティ管理装置の I D 認証手段により行う第 2 ステップと、

上記操作検知センサの判断結果、上記アクセスセンサの判断結果、および上記 I D 認証手段の I D 認証結果の少なくとも 1 つに応じて、上記セキュリティ管理装置の外部処理決定手段により複数の警報処理から 1 つを選択して外部装置に実行させる第 3 ステップとを備えていることを特徴とするセキュリティ管理方法。

条約第 19 条（1）の規定に基づく説明書

Statement

条約 19 条に基づく説明書

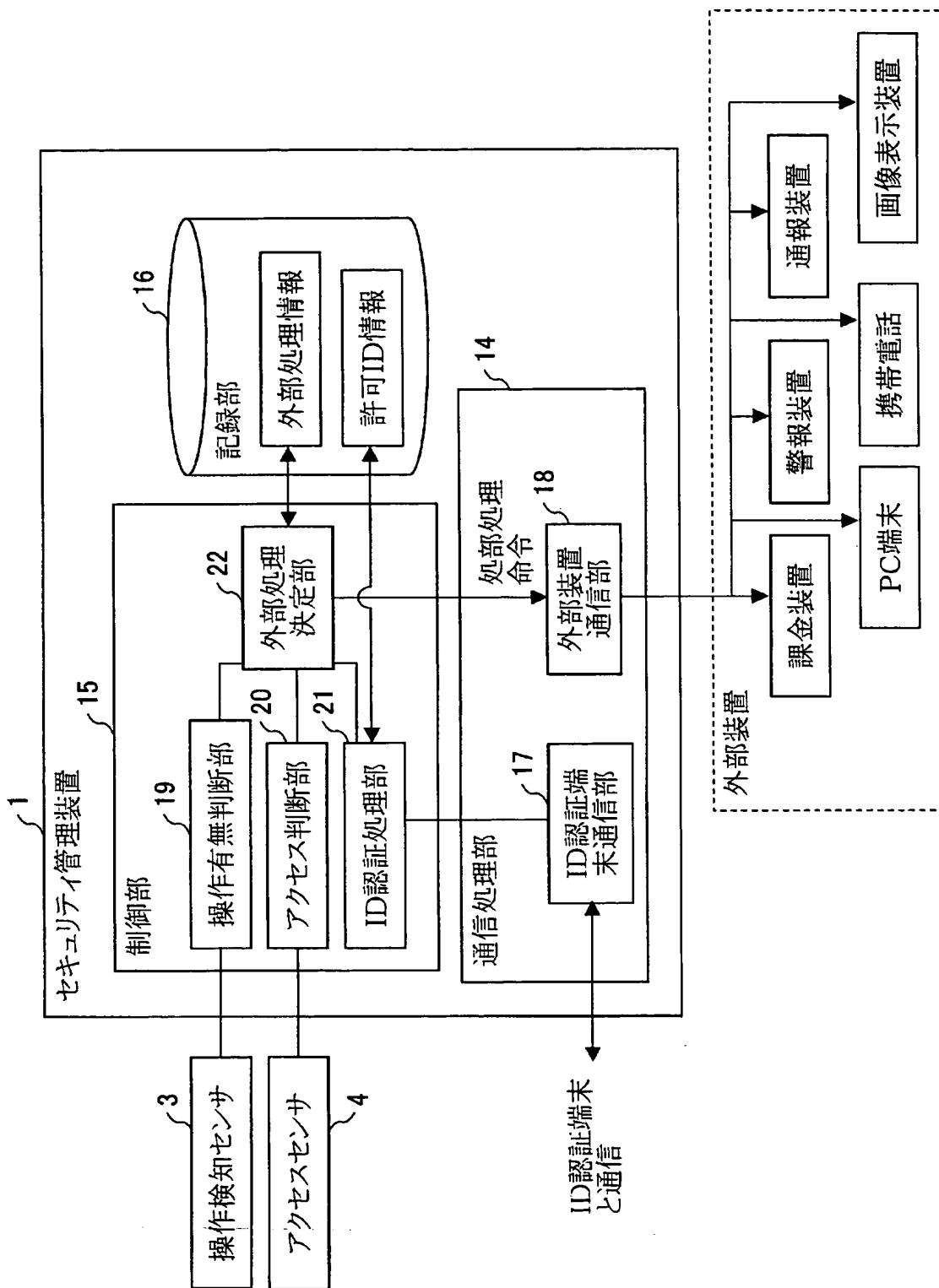
1. 本願発明と引用文献との相違点

（1）補正された請求の範囲に記載されていますように、本願発明においては、「操作検知センサの判断結果、アクセスセンサの判断結果、および I D 認証手段の I D 認証結果の少なくとも 1 つに応じて、複数のサービスから 1 つを選択して外部装置に実行」させます。

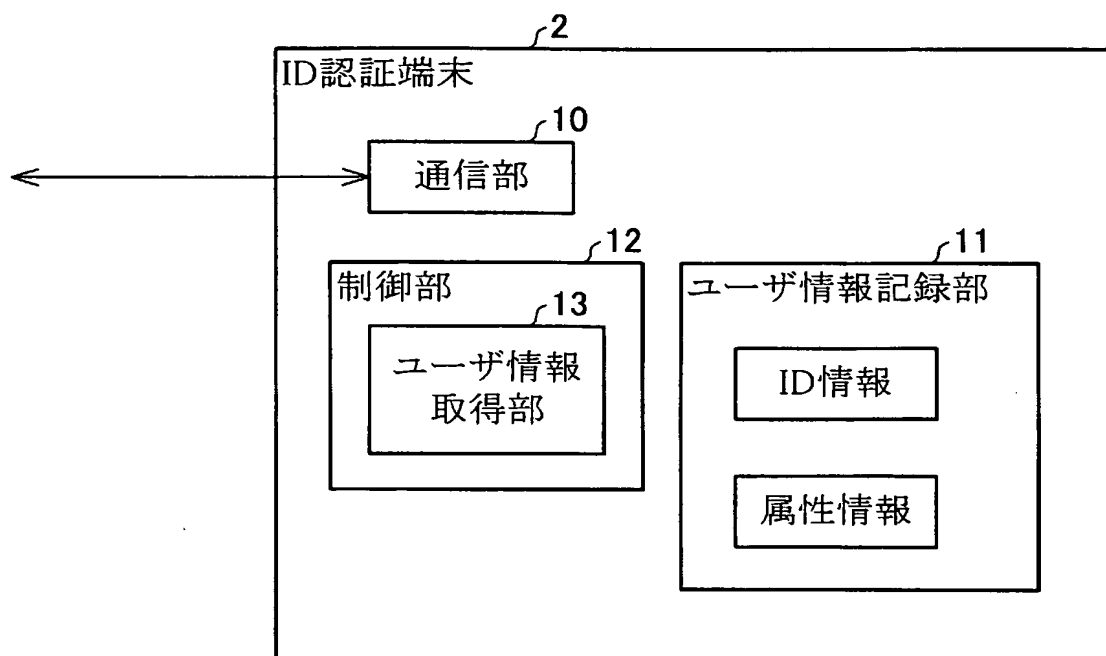
（2）これに対して、国際調査において引用された文献では、本願発明のように操作検知センサ、アクセスセンサ、および I D 認証手段の全てを備える構成については記載がありません。したがって、当該構成を有する本願発明は、引用文献に記載された発明とは異なります。

以 上

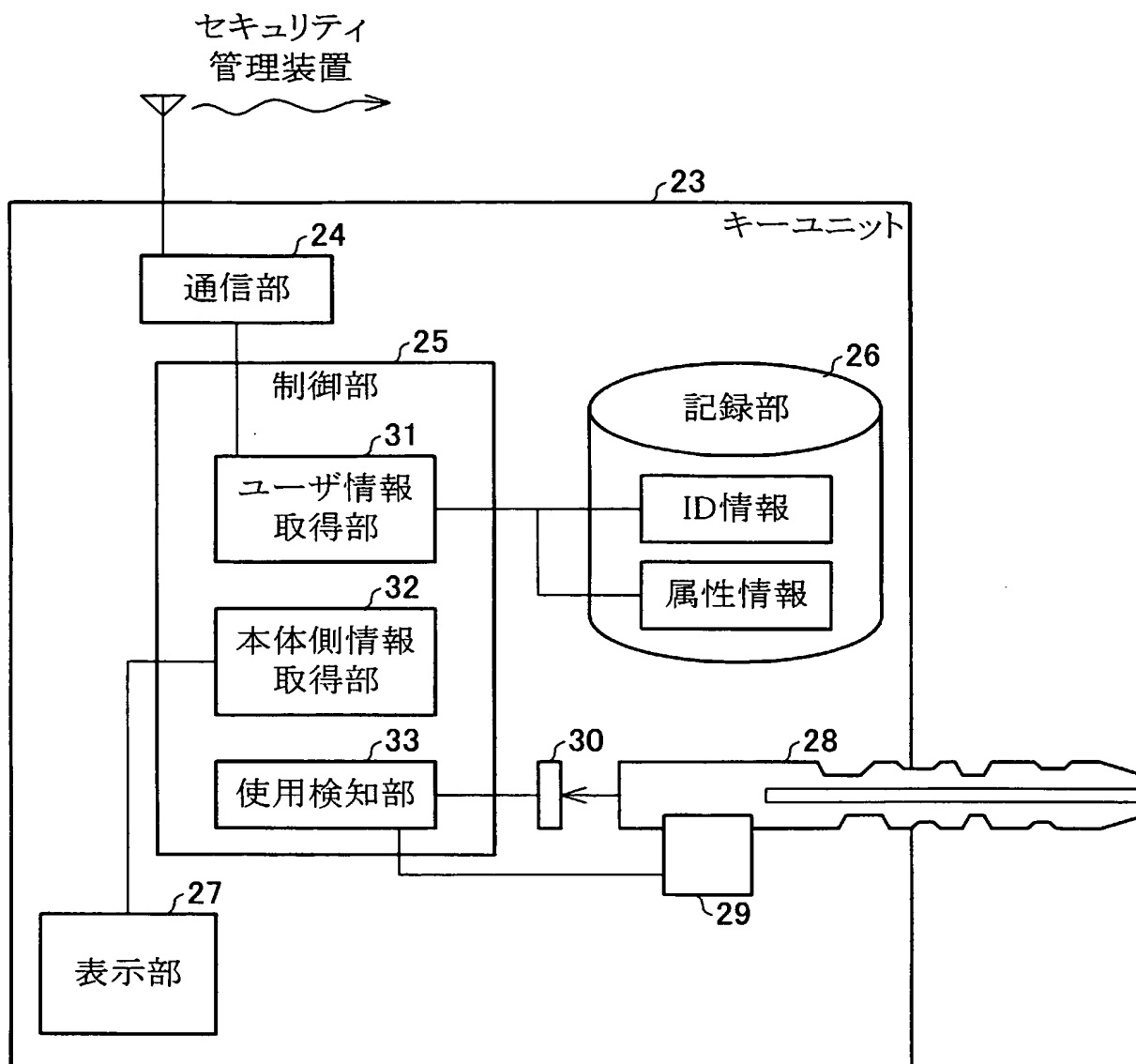
[図1]



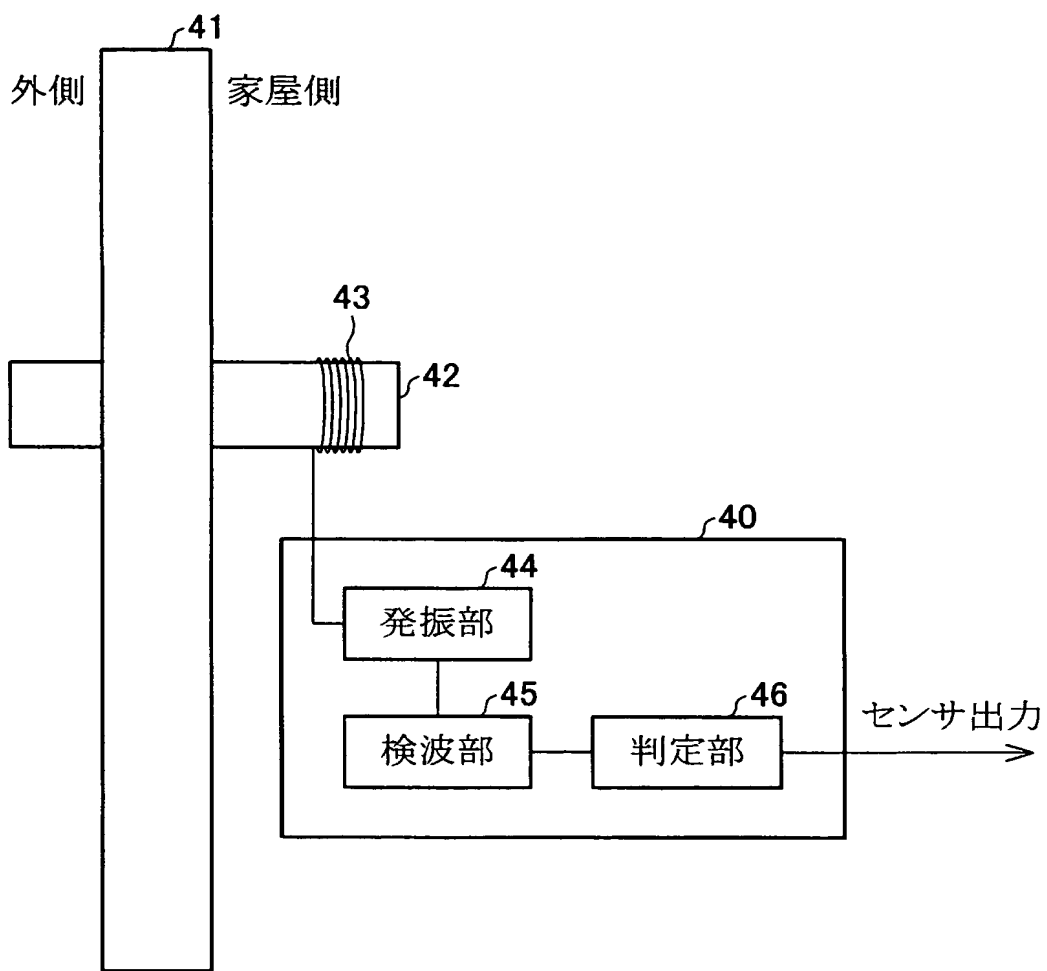
[図3]



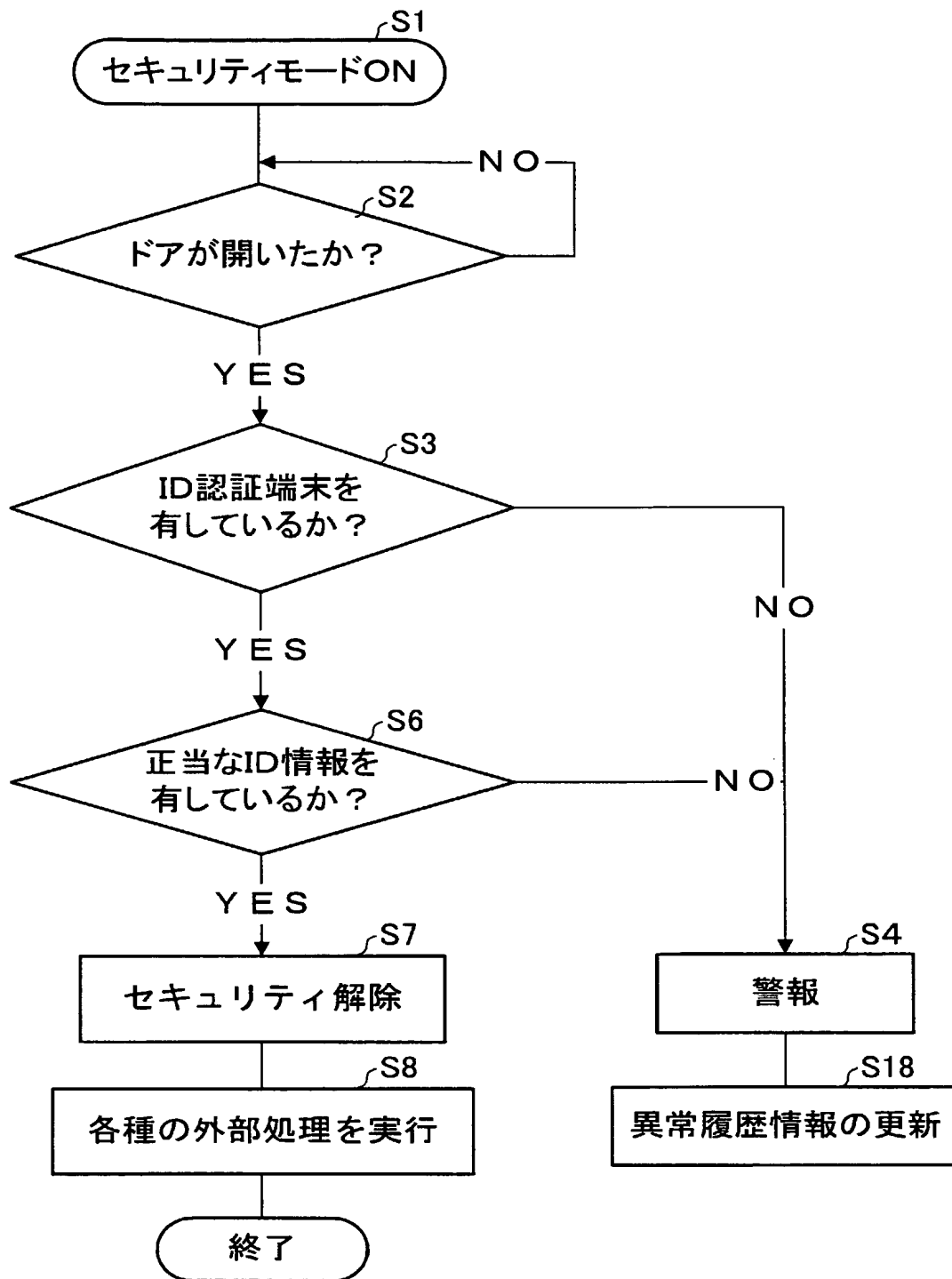
[図4]



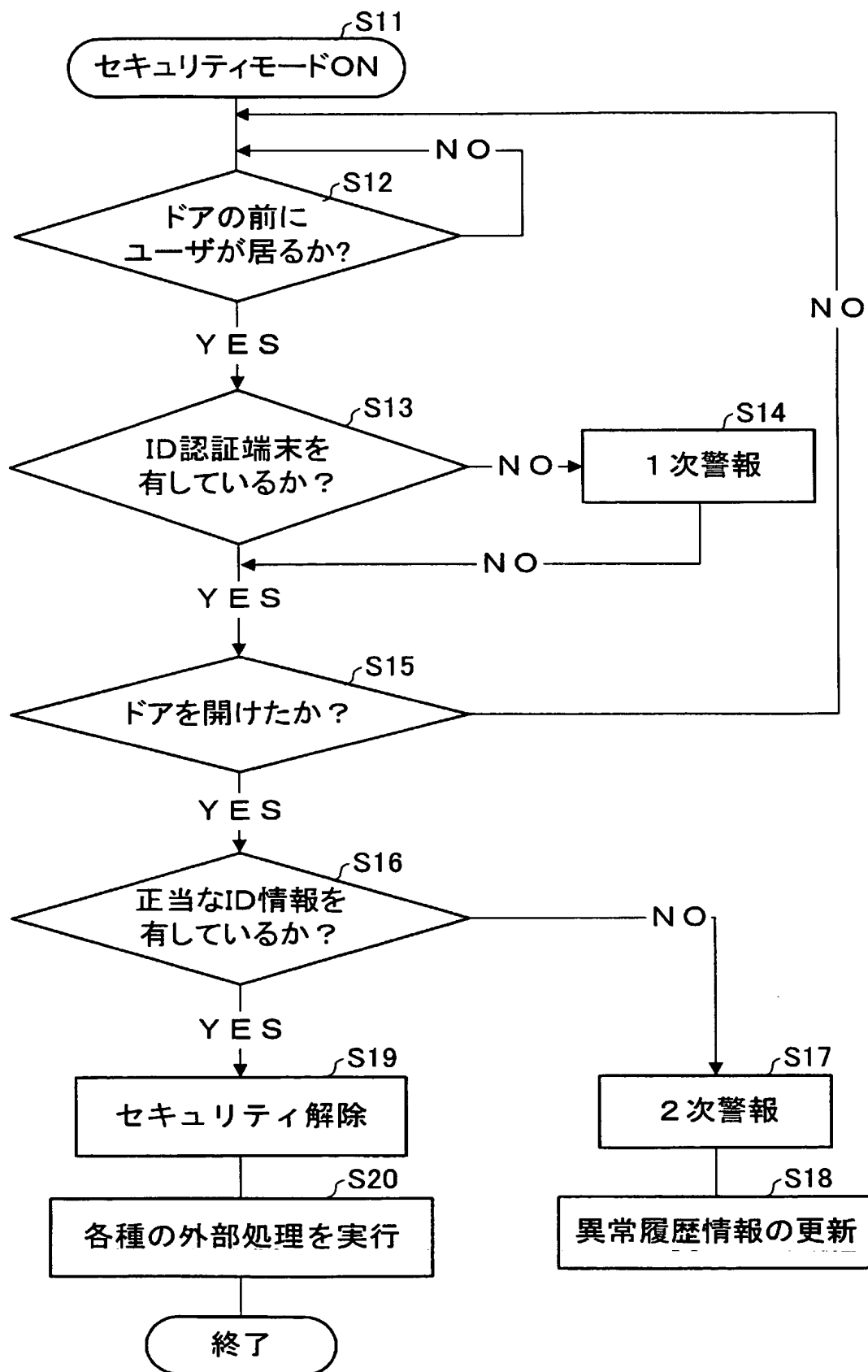
[図5]



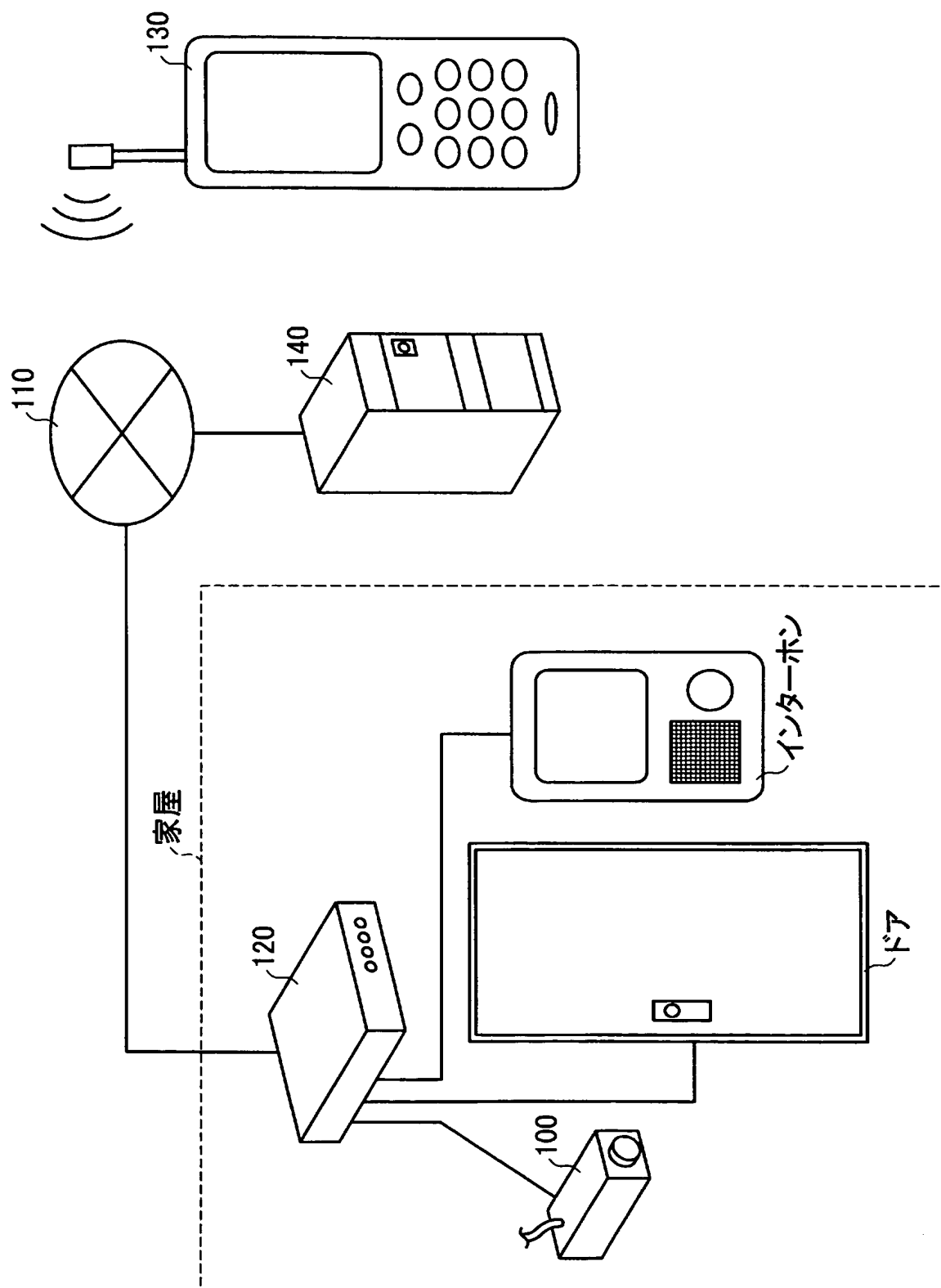
[図6]



[図7]



[図8]



[図9]

